

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-236403

(43)Date of publication of application : 02.09.2005

(51)Int.Cl.

H04L 9/32

G06F 12/14

G06F 15/00

(21)Application number : 2004-040182

(71)Applicant : TOKYO HOSO:KK

(22)Date of filing : 17.02.2004

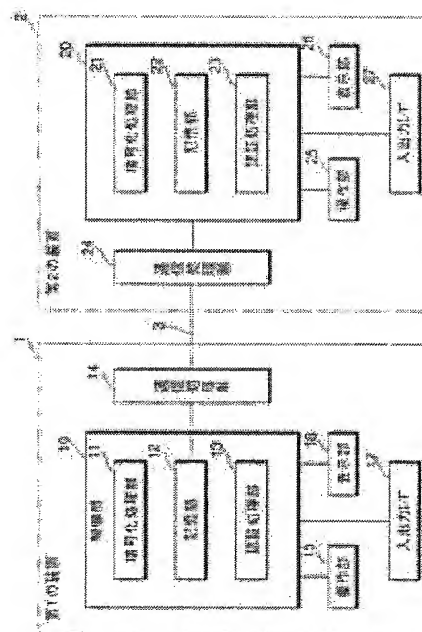
(72)Inventor : SASADA MASAOKI

(54) METHOD AND SYSTEM FOR ELECTRONIC AUTHENTICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic authentication method and an authentication system capable of easily performing the procedure of mutual authentication of electronic information at a low cost between parties concerned without intervention of a third party organization.

SOLUTION: Both a first device (1) and a second device (2) perform first encryption for a plain text by using an encryption key based on an encryption system having exchangeability, and provide and receive the generated encrypted information each other. Next, both the first device (1) and the second device (2) perform second encryption for the encrypted information received from the opposite device by using an encryption key based on an encryption system having exchangeability, and each store the generated encrypted information in their own devices and provide/receive to/from the opposite device. Since both the devices each can obtain the encrypted information obtained by encrypting the information by the own device, and then encrypting by the opposite device and the encrypted information obtained by encrypting the information by the opposite device and then encrypting by the own device; the similarity of the plain texts of both the parties concerned can be authenticated by determining whether the encrypted information matches.



(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-236403

(P2005-236403A)

(43) 公開日 平成17年9月2日(2005.9.2)

(51) Int.Cl.⁷

F I

テーマコード (参考)

H 0 4 L 9/32

H 0 4 L 9/00 6 7 5 A

5 B 0 1 7

G 0 6 F 12/14

G 0 6 F 12/14 3 2 0 C

5 B 0 8 5

G 0 6 F 15/00

G 0 6 F 15/00 3 3 0 E

5 J 1 0 4

審査請求 未請求 請求項の数 8 O L (全 22 頁)

(21) 出願番号 特願2004-40182 (P2004-40182)
 (22) 出願日 平成16年2月17日(2004.2.17)

(71) 出願人 591084850
 株式会社東京放送
 東京都港区赤坂5丁目3番6号
 (74) 代理人 100079108
 弁理士 稲葉 良幸
 (74) 代理人 100080953
 弁理士 田中 克郎
 (74) 代理人 100093861
 弁理士 大賀 真司
 (72) 発明者 笹田 正明
 東京都港区赤坂5-3-6 株式会社東京
 放送内
 Fターム(参考) 5B017 AA07 BA05
 5B085 AE23 AE29 BG02 CA02 CA04
 5J104 LA02 PA07 PA10

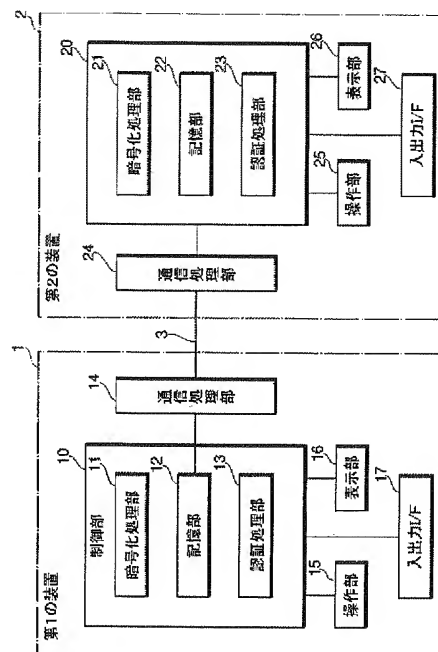
(54) 【発明の名称】 電子認証方法及び電子認証システム

(57) 【要約】

【課題】 第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことを可能とする電子認証方法及びシステムを提供すること。

【解決手段】 平文に対して、第1の装置(1)及び第2の装置(2)の双方が、可換性を有する暗号方式に基づく暗号鍵を用いて1回目の暗号化を行い、生成された暗号化情報を互いに授受する。次に第1の装置(1)及び第2の装置(2)の双方が、相手装置から受け取った暗号化情報に対して、可換性を有する暗号方式に基づく暗号鍵を用いて2回目の暗号化を行い、生成された暗号化情報を自装置に記憶すると共に相手装置と授受する。双方の装置には、自装置が暗号化してその後に相手装置が暗号化して得られた暗号化情報と、相手装置が暗号化してその後に自装置が暗号化して得られた暗号化情報とが得られるので、これらの暗号化情報の一致判定を行うことにより当事者双方の平文の同一性が認証される。

【選択図】 図1



【特許請求の範囲】**【請求項1】**

第1の装置と第2の装置との相互間において、互いが有する平文の同一性を認証する電子認証方法であって、

前記第1の装置が、前記平文に対して、可換性を有する暗号方式に基づく第1の暗号鍵を用いた暗号化処理を行って第1の暗号化情報を生成する第1ステップと、

前記第2の装置が、前記平文に対して、可換性を有する暗号方式に基づく第2の暗号鍵を用いた暗号化処理を行って第2の暗号化情報を生成する第2ステップと、

前記第1の装置が、前記第1の暗号化情報を前記第2の装置に送る第3ステップと、

前記第2の装置が、前記第2の暗号化情報を前記第1の装置に送る第4ステップと、

前記第1の装置が、前記第2の装置から取得した前記第2の暗号化情報に対して、前記第1の暗号鍵を用いた暗号化処理を行って第3の暗号化情報を生成して自装置内に記憶する第5ステップと、

前記第2の装置が、前記第1の装置から取得した前記第1の暗号化情報に対して、前記第2の暗号鍵を用いた暗号化処理を行って第4の暗号化情報を生成して自装置内に記憶する第6ステップと、

前記第1の装置が、前記第3の暗号化情報を前記第2の装置に送る第7ステップと、

前記第2の装置が、前記第4の暗号化情報を前記第1の装置に送る第8ステップと、

前記第1の装置が、自装置内に記憶した前記第3の暗号化情報と前記第2の装置から取得した前記第4の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する第9ステップと、

前記第2の装置が、自装置内に記憶した前記第4の暗号化情報と前記第1の装置から受け取った前記第3の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する第10ステップと、

を含むことを特徴とする電子認証方法。

【請求項2】

前記第3及び第4ステップにおいて、前記第1及び第2の装置のそれぞれは、前記第1及び第2の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項1に記載の電子認証方法。

【請求項3】

前記第7及び第8ステップにおいて、前記第1及び第2の装置のそれぞれは、前記第3及び第4の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項1に記載の電子認証方法。

【請求項4】

前記第1及び第2の暗号鍵は、前記第1乃至第10ステップによる一連の認証処理を行う都度に異なる使い捨て鍵である、請求項1乃至3のいずれかに記載の電子認証方法。

【請求項5】

第1の装置と第2の装置との相互間において、互いが有する平文の同一性を認証する電子認証システムであって、

前記第1及び第2の装置のそれぞれは暗号化手段、通信手段、記憶手段及び認証手段を備え、当該第1及び第2の装置が以下のように動作することを特徴とする電子認証システム。

(1) 前記第1の装置は、前記暗号化手段により、前記平文に対して、可換性を有する暗号方式に基づく第1の暗号鍵を用いた暗号化処理を行って第1の暗号化情報を生成し、当該第1の暗号化情報を前記通信手段により前記第2の装置に送る。

(2) 前記第2の装置は、前記暗号化手段により、前記平文に対して、可換性を有する暗号方式に基づく第2の暗号鍵を用いた暗号化処理を行って第2の暗号化情報を生成し、当該第2の暗号化情報を前記通信手段により前記第1の装置に送る。

(3) 前記第1の装置は、前記第2の装置から取得した前記第2の暗号化情報に対して、

前記暗号化手段により前記第1の暗号鍵を用いた暗号化処理を行って第3の暗号化情報を生成して前記記憶手段に記憶するとともに、当該第3の暗号化情報を前記通信手段により前記第2の装置に送る。

(4) 前記第2の装置は、前記第1の装置から取得した前記第1の暗号化情報に対して、前記第2の暗号鍵を用いた暗号化処理を行って第4の暗号化情報を生成して前記記憶手段に記憶するとともに、当該第4の暗号化情報を前記通信手段により前記第1の装置に送る。

(5) 前記第1の装置は、前記認証手段により、前記記憶手段に記憶した前記第3の暗号化情報と前記第2の装置から取得した前記第4の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する。

(6) 前記第2の装置は、前記認証手段により、前記記憶手段に記憶した前記第4の暗号化情報と前記第1の装置から取得した前記第3の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する。

【請求項6】

前記第1の装置の前記通信手段と前記第2の装置の前記通信手段は、それぞれ前記第1及び第2の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項5に記載の電子認証システム。

【請求項7】

前記第1の装置の前記通信手段と前記第2の装置の前記通信手段は、それぞれ前記第3及び第4の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項5又は6に記載の電子認証システム。

【請求項8】

前記第1及び第2の暗号鍵は、認証処理を行う都度に異なる使い捨て鍵である、請求項5乃至7のいずれかに記載の電子認証システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、複数の当事者間で電子情報について相互認証を行うための電子認証技術に関する。

【背景技術】

【0002】

情報化社会の進展により、従来、紙などの物理的な媒体を用いてやり取りされていた文書（例えば各種の契約書、受領書等）が電子情報に置き換えられつつある。例えば、配送業者が利用者に種々の配送品を届けるような場合を考えると、従来の紙の受領書を介した受領手続きが電子情報の受領書に置き換えられる。またインターネットを介したショッピング等でも同様であり、従来は郵送やファクシミリによって授受されていた注文書が電子情報の注文書に置き換えられる。このように、従来の紙などの物理的媒体を電子情報に代替するには、当該電子情報が複製、改ざん等の不正処理に強いものであることが必要である。このような複数の当事者間における文書等の電子情報の授受手続きにおいて互いの保有する電子情報の認証（正当性の確認）を行う方法の1つとして、信頼の高い第三者による外部認証機関を介した電子情報の授受が知られている。このような従来技術は、例えば特開2002-132145号公報などの文献に開示されている。

【0003】

【特許文献1】特開2002-132145号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

ところで、上述した第三者認証機関を利用する電子認証では、より安全性の高い認証を行うことが可能となるが、当事者の双方が事前に認証機関への登録手続きが必要であったり、電子情報のやり取りを行う毎にネットワークを介して認証機関へ接続する必要がある

など、利用者の利便性に欠けると共にコストが高くつくという不都合がある。特に、上述したような受領書や発注書等の授受手続きのように、日常生活に密着した事柄に関する電子認証については、より低コストで簡便に認証手続きを行なえることが望ましい。

【0005】

そこで、本発明は、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことを可能とする電子認証方法及びシステムを提供することを目的とする。

【課題を解決するための手段】

【0006】

第1の態様の本発明は、第1の装置と第2の装置との相互間において、互いが有する平文の同一性を認証する電子認証方法であって、上記第1の装置が、上記平文に対して、可換性を有する暗号方式に基づく第1の暗号鍵を用いた暗号化処理を行って第1の暗号化情報を生成する第1ステップと、上記第2の装置が、上記平文に対して、可換性を有する暗号方式に基づく第2の暗号鍵を用いた暗号化処理を行って第2の暗号化情報を生成する第2ステップと、上記第1の装置が、上記第1の暗号化情報を上記第2の装置に送る第3ステップと、上記第2の装置が、上記第2の暗号化情報を上記第1の装置に送る第4ステップと、上記第1の装置が、上記第2の装置から取得した上記第2の暗号化情報に対して、上記第1の暗号鍵を用いた暗号化処理を行って第3の暗号化情報を生成して自装置内に記憶する第5ステップと、上記第2の装置が、上記第1の装置から取得した上記第1の暗号化情報に対して、上記第2の暗号鍵を用いた暗号化処理を行って第4の暗号化情報を生成して自装置内に記憶する第6ステップと、上記第1の装置が、上記第3の暗号化情報を上記第2の装置に送る第7ステップと、上記第2の装置が、上記第4の暗号化情報を上記第1の装置に送る第8ステップと、上記第1の装置が、自装置内に記憶した上記第3の暗号化情報と上記第2の装置から取得した上記第4の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する第9ステップと、上記第2の装置が、自装置内に記憶した上記第4の暗号化情報と上記第1の装置から受け取った上記第3の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する第10ステップと、を含むことを特徴とする電子認証方法である。

【0007】

ここで、本明細書において「平文」とは、暗号化処理などの処理がなされていない状態の電子情報（電子データ）をいい、各種の契約書、受領書その他の文書データが含まれる。また「可換性を有する暗号方式」とは、暗号化の対象となる電子情報に対して、少なくとも2回の暗号化処理を行う場合において、当該暗号化処理の1回目に行うものと2回目に行うものとで順番を相互に入れ替えても結果が同じとなるものをいう。

【0008】

かかる方法では、平文に対して、第1の装置及び第2の装置の双方が、可換性を有する暗号方式に基づく暗号鍵を用いて1回目の暗号化を行い、生成された暗号化情報（第1又は第2の暗号化情報）を互いに授受する。次に、第1の装置及び第2の装置の双方が、相手装置から受け取った暗号化情報に対して、可換性を有する暗号方式に基づく暗号鍵を用いて2回目の暗号化を行い、生成された暗号化情報（第3又は第4の暗号化情報）を自装置に記憶すると共に相手装置と授受する。この手順により、双方の装置には、自装置が暗号化してその後に相手装置が暗号化して得られた暗号化情報と、相手装置が暗号化してその後に自装置が暗号化して得られた暗号化情報とが得られる。よって、これらの暗号化情報の一致判定を行うことにより当事者双方の平文の同一性を認証することができる。したがって、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。

【0009】

また、上記第3及び第4ステップにおいて、上記第1及び第2の装置のそれぞれは、上記第1及び第2の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。

【0010】

また、上記第7及び第8ステップにおいて、上記第1及び第2の装置のそれぞれは、上記第3及び第4の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。

【0011】

また、上記第1及び第2の暗号鍵は、上記第1乃至第10ステップによる一連の認証処理を行う都度に異なる使い捨て鍵であることが好ましい。

【0012】

第2の態様の本発明は、第1の装置と第2の装置との相互間において、互いが有する平文の同一性を認証する電子認証システムであって、上記第1及び第2の装置のそれぞれは暗号化手段、通信手段、記憶手段及び認証手段を備え、当該第1及び第2の装置が以下のように動作することを特徴とする電子認証システムである。すなわち、

(1) 上記第1の装置は、上記暗号化手段により、上記平文に対して、可換性を有する暗号方式に基づく第1の暗号鍵を用いた暗号化処理を行って第1の暗号化情報を生成し、当該第1の暗号化情報を上記通信手段により上記第2の装置に送る。

(2) 上記第2の装置は、上記暗号化手段により、上記平文に対して、可換性を有する暗号方式に基づく第2の暗号鍵を用いた暗号化処理を行って第2の暗号化情報を生成し、当該第2の暗号化情報を上記通信手段により上記第1の装置に送る。

(3) 上記第1の装置は、上記第2の装置から取得した上記第2の暗号化情報に対して、上記暗号化手段により上記第1の暗号鍵を用いた暗号化処理を行って第3の暗号化情報を生成して上記記憶手段に記憶するとともに、当該第3の暗号化情報を上記通信手段により上記第2の装置に送る。

(4) 上記第2の装置は、上記第1の装置から取得した上記第1の暗号化情報に対して、上記第2の暗号鍵を用いた暗号化処理を行って第4の暗号化情報を生成して上記記憶手段に記憶するとともに、当該第4の暗号化情報を上記通信手段により上記第1の装置に送る。

(5) 上記第1の装置は、上記認証手段により、上記記憶手段に記憶した上記第3の暗号化情報と上記第2の装置から取得した上記第4の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する。

(6) 上記第2の装置は、上記認証手段により、上記記憶手段に記憶した上記第4の暗号化情報と上記第1の装置から取得した上記第3の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する。

【0013】

かかるシステムでは、平文に対して、第1の装置及び第2の装置の双方が、可換性を有する暗号方式に基づく暗号鍵を用いて1回目の暗号化を行い、生成された暗号化情報(第1又は第2の暗号化情報)を互いに授受する。次に、第1の装置及び第2の装置の双方が、相手装置から受け取った暗号化情報に対して、可換性を有する暗号方式に基づく暗号鍵を用いて2回目の暗号化を行い、生成された暗号化情報(第3又は第4の暗号化情報)を自装置に記憶すると共に相手装置と授受する。これにより、双方の装置には、自装置が暗号化してその後に相手装置が暗号化して得られた暗号化情報と、相手装置が暗号化してその後に自装置が暗号化して得られた暗号化情報とが得られる。よって、これらの暗号化情報の一致判定を行うことにより当事者双方の平文の同一性を認証することができる。したがって、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。

【0014】

また、上記第1の装置の上記通信手段と上記第2の装置の上記通信手段は、それぞれ上記第1及び第2の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。

【0015】

また、上記第1の装置の上記通信手段と上記第2の装置の上記通信手段は、それぞれ上

記第3及び第4の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。

【0016】

また、上記第1及び第2の暗号鍵は、認証処理を行う都度に異なる使い捨て鍵であることが好ましい。

【発明の効果】

【0017】

本発明によれば、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。

【発明を実施するための最良の形態】

【0018】

以下、本発明の実施の形態について図面を参照しながら説明する。

【0019】

始めに本実施形態において使用される「可換性のある暗号方式」について説明する。一例として離散対数問題を利用する方法について説明する。

【0020】

認証対象となる平文をTとし、この平文TをAとBの二者間（二装置間）で認証する場合を考える。一方のAが有する平文Tを以後「Ta」と表記し、他方のBが有する平文Tを以後「Tb」と表記する。

【0021】

まず、大きな素数Pを選ぶ。Pはシステムに共通とする。

【0022】

今、Aは鍵 X_A （ $0 \leq X_A < P-1$ ）を生成し、下記計算を行う。

【0023】

【数1】

$$y_A \equiv T a^{X_A} \bmod P$$

【0024】

y_A から X_A を求めるのは離散対数計算の困難さから難しいので、Taから y_A を生成できるのは X_A を知っているAだけである。Aはこの計算結果 y_A をBに送る。

【0025】

Bは鍵 X_B （ $0 \leq X_B < P-1$ ）を生成し、下記計算を行う。

【0026】

【数2】

$$y_B \equiv T b^{X_B} \bmod P$$

【0027】

上記と同様に、 y_B から X_B を求めるのは離散対数計算の困難さから難しいので、Tbから y_B を生成できるのは X_B を知っているBだけである。Bはこの計算結果 y_B をAに送る。

【0028】

Aは y_B に対して、自らの鍵 X_A を用いて、下記yを計算する。

【0029】

【数3】

$$y = y_B^{X_A} = T b^{X_B \cdot X_A} \bmod P$$

【0030】

Bは y_A に対して、自らの鍵 X_B を用いて、下記 y を計算する。

【0031】

【数4】

$$y = y_A^{X_B} = T_a^{X_A \cdot X_B} \bmod P$$

【0032】

このとき、Aが求めた y とBが求めた y とが等しければ、下記の式が成り立ち、 $T_a = T_b$ が証明される。

【0033】

【数5】

$$y = T_b^{X_B \cdot X_A} = T_b^{X_A \cdot X_B} = T_a^{X_A \cdot X_B} \bmod P$$

【0034】

従来のデジタル署名では、公開鍵暗号であるRSA暗号を用いて上記と同様な効果を有する証明を行っていた。これに対して、本実施形態では、公開鍵を利用せず、当事者間だけで文書の一致を検証することに特徴がある。ただし、上記素数Pについては、当事者の相互間で同じ値を使用する必要がある。電子印鑑等の認証装置に本実施形態の認証方式を採用する場合であれば、例えば当該電子印鑑等の製造者が素数Pを定める。

【0035】

本実施形態では、以上に説明したような可換性を有する暗号方式を利用して、二者間のみで信頼性の高い認証を可能としている。以下、かかる暗号方式を採用したシステムの実施の形態について更に詳細に説明する。

【0036】

図1は、本発明を適用した一実施形態の電子認証システムの構成を説明する図である。図1に示す電子認証システムは、通信媒体3を介して相互に接続された第1の装置1と第2の装置2とを含んで構成される。本システムでは、第1及び第2の装置の相互間において、互いが有する平文の同一性についての認証が行われる。

【0037】

第1の装置1は、当該装置の全体動作を制御する制御部10と、外部装置との情報通信処理を担う通信処理部（通信手段）14と、各種の操作指示を入力するために用いられる操作部15と、第1の装置1の動作状態等を表示するための表示部16と、外部メモリ等との間での情報の授受を行うための入出力インタフェース（I/F）17と、を含んで構成される。

【0038】

制御部10は、例えばCPU、ROM、RAMなどを含んで構成されるいわゆるコンピュータと、当該コンピュータに所定の処理を行わせ、或いは所定の処理を実現する手段として機能させるためのプログラムとが協働して実現される。この制御部10は、暗号化処理部11、記憶部12、認証処理部13を含む。

【0039】

暗号化処理部（暗号化手段）11は、上述した平文或いはその他の電子情報に対して、所定の暗号方式による暗号化を行うものである。特に本実施形態では、この暗号化処理部11において用いる暗号方式として、可換性を有する暗号方式を採用している。

【0040】

記憶部（記憶手段）12は、上述した平文或いはその他の電子情報を記憶するものである。

【0041】

認証処理部（認証手段）13は、自装置（第1の装置1）が有する平文と、相手側装置（第2の装置2）の有する平文とが同一なものであるか否か、すなわち平文の同一性につ

いての認証を行うものである。

【0042】

第2の装置2は、当該装置の全体動作を制御する制御部20と、外部装置との情報通信処理を担う通信処理部（通信手段）24と、各種の操作指示を入力するために用いられる操作部25と、第2の装置2動作状態等を表示するための表示部26と、外部メモリ等との間での情報の授受を行うための入出力インタフェース（I/F）27と、を含んで構成される。また制御部20は、暗号化処理部（暗号化手段）21、記憶部（記憶手段）22、認証処理部（認証手段）23を含む。この第2の装置2の構成は上述した第1の装置と同様であるので、各構成要素についての詳細な説明は省略する。

【0043】

本実施形態の電子認証システムはこのような構成を有しており、次に認証処理の詳細について説明する。

【0044】

図2は、本実施形態の電子認証システムにおける認証処理の手順を説明するフローチャートである。本フローチャートでは、第1の装置1と第2の装置2のそれぞれの動作内容が並行して示されている。

【0045】

まず、第1の装置1と第2の装置2とが同一の平文Tを取得する（ステップS100、S200）。各装置における平文の取得は、例えば入出力I/F17、27のそれぞれを介して行われる。なお、説明の便宜上、以下では、第1の装置1が取得した平文を「Ta」、第2の装置が取得した平文を「Tb」とそれぞれ表記する。

【0046】

次に、第1の装置1は、平文Taに対して、可換性を有する暗号方式に基づく第1の暗号鍵Kaを用いた暗号化処理を行って第1の暗号化情報（Ta）Kaを生成する（ステップS101）。より具体的には当該処理は暗号化処理部11によって行われる。

【0047】

また、第2の装置は、平文Tbに対して、可換性を有する暗号方式に基づく第2の暗号鍵Kbを用いた暗号化処理を行って第2の暗号化情報（Tb）Kbを生成する（ステップS201）。より具体的には当該処理は暗号化処理部21によって行われる。

【0048】

ここで、上記第1の暗号鍵Ka及び第2の暗号鍵Kbは、それぞれ一連の認証処理を行う都度に異なる使い捨て鍵であることが望ましい。

【0049】

次に、第1の装置1は、第1の暗号化情報（Ta）Kaを第2の装置に送信する（ステップS102）。より具体的には当該処理は通信処理部14によって行われる。

【0050】

また、第2の装置2は、第2の暗号化情報（Tb）Kbを第1の装置1に送信する（ステップS202）。より具体的には当該処理は通信処理部24によって行われる。

【0051】

第1の装置1は、第2の装置から送られた第2の暗号化情報（Tb）Kbを受信する。（ステップS103）。より具体的には当該処理は通信処理部14によって行われる。また、第2の装置2は、第1の装置から送られた第1の暗号化情報（Ta）Kaを受信する。（ステップS203）。より具体的には当該処理は通信処理部24によって行われる。

【0052】

ここで、第1及び第2の暗号化情報の送信及び受信は、当該第1及び第2の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが望ましい。例えば、本実施形態では、第1の装置1と第2の装置2との間で、互いに1ビットずつ交互にデータを送り合うようにする。これにより、仮に第1及び第2の暗号化情報の送信／受信時にこれらの暗号化情報を来た方向に折り返す不正操作を回避することが可能となる。なお、部分情報のデータ量は1ビットずつに限定されるものではなく、任意に変更可能である。

【0053】

次に、第1の装置1は、第2の装置2から取得した第2の暗号化情報(Tb) Kbに対して、第1の暗号鍵Kaを用いた暗号化処理を行って第3の暗号化情報(Tb) KbKaを生成して自装置内に記憶する(ステップS104)。より具体的には、第3の暗号化情報の生成は暗号化処理部11により行われ、当該第3の暗号化情報の記憶は記憶部12により行われる。

【0054】

また、第2の装置2は、第1の装置1から取得した第1の暗号化情報(Ta) Kaに対して、第2の暗号鍵Kbを用いた暗号化処理を行って第4の暗号化情報(Ta) KaKbを生成して自装置内に記憶する(ステップS204)。より具体的には、第4の暗号化情報の生成は暗号化処理部21により行われ、当該第4の暗号化情報の記憶は記憶部22により行われる。

【0055】

次に、第1の装置1は、第3の暗号化情報(Tb) KbKaを第2の装置2に送信する(ステップS105)。より具体的には当該処理は通信処理部14によって行われる。

【0056】

また、第2の装置2は、第4の暗号化情報(Ta) KaKbを第1の装置1に送信する(ステップS205)。より具体的には当該処理は通信処理部24によって行われる。

【0057】

第1の装置1は、第2の装置から送られた第4の暗号化情報(Ta) KaKbを受信する。(ステップS106)。より具体的には当該処理は通信処理部14によって行われる。また、第2の装置2は、第1の装置から送られた第3の暗号化情報(Tb) KbKaを受信する。(ステップS206)。より具体的には当該処理は通信処理部24によって行われる。

【0058】

ここで、第3及び第4の暗号化情報の送信及び受信は、当該第3及び第4の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが望ましい。例えば、本実施形態では、第1の装置1と第2の装置2との間で、互いに1ビットずつ交互にデータを送り合うようにする。これにより、仮に第3及び第4の暗号化情報の送信/受信時にこれらの暗号化情報を来た方向に折り返す不正操作を回避することが可能となる。なお、部分情報のデータ量は1ビットずつに限定されるものではなく、任意に変更可能である。

【0059】

次に、第1の装置1は、自装置内に記憶した第3の暗号化情報(Tb) KbKaと第2の装置2から取得した第4の暗号化情報(Ta) KaKbとが一致するか否かを判定する(ステップS107)。より具体的には、当該判定は認証処理部13によって行われる。可換性を有する暗号方式を採用しているので、第1の装置1が有する平文Taと第2の装置2が有する平文Tbのいずれか或いは両方が、何らかの方法で改ざん、偽造等されていなければ、(Tb) KbKa = (Ta) KaKbとなる。よって、第3及び第4の暗号化情報の一致判断を行えば、平文の同一性について認証できる。

【0060】

第3の暗号化情報と第4の暗号化情報とが一致する場合には、ステップS107で肯定判断(YES)がなされ、第1の装置1は、平文が同一、すなわち平文の同一性が有効であると認証する(ステップS108)。より具体的には当該認証は認証処理部13により行われる。

【0061】

また、第3の暗号化情報と第4の暗号化情報とが一致しない場合には、ステップS107で否定判断(NO)がなされ、第1の装置1は、平文の同一性が有効ではないと認証して一連の処理を終了する。

【0062】

なお、平文の同一性についての認証結果は、例えば表示部16を介して使用者に提示さ

れ、或いは相手側である第2の装置2に通知される。

【0063】

また、第2の装置2は、自装置内に記憶した第4の暗号化情報(Ta)KaKbと第1の装置1から取得した第3の暗号化情報(Tb)KbKaとが一致するか否かを判定する(ステップS207)。より具体的には、当該判定は認証処理部23によって行われる。可換性を有する暗号方式を採用しているため、第1の装置1が有する平文Taと第2の装置2が有する平文Tbのいずれか或いは両方が、何らかの方法で改変、偽造等されていなければ、(Ta)KaKb=(Tb)KbKaとなる。よって、第3及び第4の暗号化情報の一致判断を行えば、平文の同一性について認証できる。

【0064】

第4の暗号化情報と第3の暗号化情報とが一致する場合には、ステップS207で肯定判断(YES)がなされ、第2の装置2は、平文が同一、すなわち平文の同一性が有効であると認証する(ステップS208)。より具体的には当該認証は認証処理部23におり行われる。

【0065】

また、第4の暗号化情報と第3の暗号化情報とが一致しない場合には、ステップS207で否定判断(NO)がなされ、第2の装置2は、平文の同一性が有効ではないと認証して一連の処理を終了する。

【0066】

なお、平文の同一性についての認証結果は、例えば表示部26を介して使用者に提示され、或いは相手側である第1の装置1に通知される。

【0067】

このように、本実施形態では、平文に対して当事者双方の装置がまず1回目の暗号化を行って生成した暗号化情報を互いに授受し、次に相手装置から受け取った暗号化情報に対して更に2回目の暗号化を行って生成した暗号化情報を自装置に記憶すると共に相手装置と授受する。この2回の暗号化がなされることにより、双方の装置には、(1)まず自装置が暗号化し、その後相手装置が暗号化して得られた暗号化情報と、(2)まず相手装置が暗号化し、その後自装置が暗号化して得られた暗号化情報とが得られる。可換性を有する暗号方式を採用していることから、上記(1)、(2)の暗号化情報は、原理的に一致するので、当該暗号化情報についての一致判定を行うことにより、当事者双方が有する平文の同一性を認証することができる。したがって、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。

【0068】

次に、上述した電子認証システムの応用例と当該システムに用いられる電子印鑑(電子認証装置)についての具体例を説明する。

【0069】

図3は、電子印鑑の具体例について説明する図(斜視図)である。本例の電子印鑑は、例えばPCMCIAカードに準拠した入出力インタフェースを有するカード状の電子印鑑であり、その内部に上述した実施形態にかかる第1の装置1又は第2の装置2と同等の構成を備えている。

【0070】

図3に示す電子印鑑100は、操作キー(数字キー)101、ランプ102~105、カメラユニット106、液晶表示部107、入出力インタフェース108を含んで構成されている。

【0071】

操作キー101は、例えば1~9の数字キー等を含むものであり、操作指示の入力に用いられる。当該操作キー101は、上述した操作部15又は25に対応するものである。

【0072】

ランプ102~105は、電子印鑑の動作状態、より詳細には認証結果に関する表示を行うためのものである。各ランプの点灯状態を認証結果との対応の詳細については後述す

る。なお、これらのランプ102～105と液晶表示部107とが、上述した表示部16又は26に対応している。

【0073】

カメラユニット106は、電子印鑑100を用いる使用者を撮像し、画像データを得るためのものである。カメラユニット106による撮像タイミングや得られた画像データの用途等の詳細については後述する。

【0074】

液晶表示部107は、電子印鑑の動作状態について、ランプ102等により表現し切れない詳細な情報を使用者に伝えるための文字や画像等を表示するものである。

【0075】

入出力インタフェース108は、PCMCIAカードの規格に準拠したものであり、例えばパーソナルコンピュータ等の外部機器と電子印鑑100とを接続し、データ通信を行うためのものである。

【0076】

本例の電子印鑑100はこのような構成を備えると共に、上述した第1又は第2の装置に相当する機能を備えており、次に当該電子印鑑100を使用した電子認証手続きの例について説明する。以下では、例えば消費者Aが宅配業者Bから配送品を受け取る際に、受け取りの確認を行う文書である受領書を電子情報（平文）により用意し、当該受領書に対して両当事者A、Bが互いに電子印鑑を用いて押印する場合を想定して説明する。

【0077】

ここで、以降の説明に用いるいくつかの記号、略号について定義する。

- (1) A、B：それぞれ消費者と宅配業者である。
- (2) 電子印鑑100A：消費者Aが使用する電子印鑑である。
- (3) 電子印鑑100B：宅配業者Bが使用する電子印鑑である。
- (4) T：A、Bが合意した内容を含み、認証の対象となる文書（平文）であり本例では受領書である。押印が終わったあとに電子印鑑100A及び100Bに同じものが保存される。
- (5) Tf：正規の平文Tに代わるべく悪意の他者（A又はBも当該他者となり得る）が改ざんした平文である。
- (6) スタンプID：各電子印鑑に固有の識別番号であり、電子印鑑の製造時に設定される不変の番号である。電子印鑑100AのスタンプIDを「IDA」、電子印鑑100BのスタンプIDを「IDB」とする。
- (7) IncrN：使用履歴に応じて変化する番号であり、予め設定された規則（ロジック）により変化する。電子印鑑100Aの番号を「IncrNA」、電子印鑑100Bの番号を「IncrNB」とする。このIncrNは、メーカーにより特定の変化をするように設定される数であり、同じ数は2度と現れない。メーカーは、依頼があればその電子印鑑が発生し得るIncrNであるか否かを明らかにできる。
- (8) Incr：IncrNを暗号化して変化のロジックを見えなくしたものである。電子印鑑100Aの番号を「IncrA」、電子印鑑100Bの番号を「IncrB」とする。本例では、所定の暗号鍵（後述する）により暗号化した数をIncrとする。
- (9) TID：記録されている自分と相手のそれぞれのスタンプID及びIncrの計4つによって特定される情報であり、システム内で一意である。
- (10) TIDA：IDAとIncrAとの組み合わせである。電子印鑑100A内で一意である。
- (11) TIDB：IDBとIncrBとの組み合わせである。電子印鑑100B内で一意である。
- (12) Text：当事者A、Bが合意した内容である。
- (13) Textf：当事者の一方がTextの内容を改ざんしたものである。
- (14) Ta：当事者Aが正しい（有効）として電子印鑑100A内に記録し、認証に使う文書である。

(15) T b : 当事者 B が正しい (有効) として電子印鑑 1 0 0 B 内に記録し、認証に使う文書である。

(16) K t : 電子印鑑のメーカ (製造者) と通信するとき使用する暗号鍵である。鍵毎に固有で不変であり、メーカが生成して各電子印鑑に設定する。電子印鑑 1 0 0 A の鍵を「K t a」、電子印鑑 1 0 0 B の鍵を「K t b」とする。

(17) K i n c r : 上述した I n c r を暗号化するための鍵であり、電子印鑑の使用に先立って、印鑑内部の乱数発生装置によって生成される。誰にも知られることがないものである。電子印鑑 1 0 0 A の鍵を「K i n c r A」、電子印鑑 1 0 0 B の鍵を「K i n c r B」とする。

(18) K : 認証時に、認証内容を暗号化して交換する際に用いる鍵であり、一回限りの使い捨ての鍵である。電子印鑑 1 0 0 A の鍵を「K a」、電子印鑑 1 0 0 B の鍵を「K b」とする。

(19) ランプ L s : 押印時に正しい文書を電子印鑑の相互間で共有できたか否かを表示するためのランプである。電子印鑑 1 0 0 A のランプを「L s A」、電子印鑑 1 0 0 B のランプを「L s B」とする。上述したランプ 1 0 2 ~ 1 0 5 のいずれかがランプ L s に対応する。

(20) ランプ L i : 認証時に、電子印鑑の所有者が正しいと主張する文書が本当に正しいか否かを表示するためのランプである。電子印鑑 1 0 0 A のランプを「L i A」、電子印鑑 1 0 0 B のランプを「L i B」とする。上述したランプ 1 0 2 ~ 1 0 5 のいずれかがランプ L i に対応する。

(21) ランプ L j : 認証時に、相手が正しいと主張する文書が T と一致するか否かを表示するためのランプである。電子印鑑 1 0 0 A のランプを「L j A」、電子印鑑 1 0 0 B のランプを「L j B」とする。上述したランプ 1 0 2 ~ 1 0 5 のいずれかがランプ L j に対応する。

(22) ランプ L f : 認証時、現在送っている文書が T であるか、T a あるいは T b なのかを表示するためのランプである。このランプの点灯状態は上述したカメラユニット 1 0 6 にも写り込む。電子印鑑 1 0 0 A のランプを「L f A」、電子印鑑 1 0 0 B の鍵を「L f B」とする。上述したランプ 1 0 2 ~ 1 0 5 のいずれかがランプ L f に対応する。

(23) H u s h : テキスト、スタンプ I D 、 I n c r 、画像データに対する改ざん防止符号である。

(24) V : カメラユニット 1 0 6 により撮像され、押印相手の電子印鑑へ送られている動画画像である。電子印鑑を使用する者の顔などが含まれる。電子印鑑 1 0 0 A が相手方に送っている動画画像を V a 、電子印鑑 1 0 0 B が相手方に送っている動画画像を V b とする。

(25) V i : 上記 V を所定のタイミング (後述する) で固定した静止画像である。スタンプ I D と I n c r N とが合成されている。電子印鑑 1 0 0 A が相手方に送る静止画像を V i a とする。この V i a により、相手方の電子印鑑 1 0 0 B の使用者の顔等と、スタンプ I D (I D B) 、 I n c r N (I n c r N B) とが目視できる。電子印鑑 1 0 0 B が相手方に送る静止画像を V i b とする。この V i b により、相手方の電子印鑑 1 0 0 A の使用者の顔等と、スタンプ I D (I D A) 、 I n c r N (I n c r N A) とが目視できる。

【0078】

図 4 は、当事者のいずれも改ざん等の不正を行わない正常な状況における電子印鑑の使用時の構成例を示す図である。端末装置 1 1 0 A は当事者 A の電子印鑑 1 0 0 A を接続するための装置、端末装置 1 1 0 B は当事者 B の電子印鑑 1 0 0 B を接続するための装置であり、これらの端末装置間が所定の通信路 1 2 0 により相互に接続される。本実施形態では、図中で一点鎖線により示すように、これらの端末装置 1 1 0 A 、 1 1 0 B 及び通信路 1 2 0 の機能を備え、電子印鑑の押印に用いられる押印ユニット (伝送装置) を用いる。以下に押印手順を説明する。

【0079】

まず、電子印鑑 1 0 0 A と電子印鑑 1 0 0 B との相互間で、スタンプ I D を交換する。

【0080】

次に、合意した契約文書Tを用意し、各端末装置100A、100Bを介して電子印鑑100Aと電子印鑑100Bの双方に送り、記録させる。電子印鑑100A内にTaが記録され、電子印鑑100B内にTbが記録される。

【0081】

次に、押印状況を示す動画像Vがカメラユニット106により撮像され、相手側の電子印鑑へ送られる。静止画像Viの撮像タイミングについては相手が決定し、電子印鑑を用いて当該タイミングを指示する。

【0082】

例えば、電子印鑑100Aで撮像された動画像Vaは電子印鑑100Bへ送られ、電子印鑑100Bに備わった液晶表示部107に表示される。当該表示を見ながら、電子印鑑100Bを使用する当事者Bにより操作部101を用いて適当なタイミングが指示されると、当該指示が電子印鑑100Aに送られる。このタイミングで電子印鑑100Aは静止画像Viaを生成する。この静止画像Viaには電子印鑑100Aに対応するスタンプIDとIncrとが合成される。またこのとき、電子印鑑100Aは、スタンプID等を合成する前の静止画像（或いは動画像でもよい）を自装置内に保存する。

【0083】

同様に、電子印鑑100Bで撮像された動画像Vbは電子印鑑100Aへ送られ、電子印鑑100Aに備わった液晶表示部107に表示される。当該表示を見ながら、電子印鑑100Aを使用する当事者Aにより操作部101を用いて適当なタイミングが指示されると、当該指示が電子印鑑100Bに送られる。このタイミングで電子印鑑100Bは静止画像Viaを生成する。この静止画像Viaには電子印鑑100Bに対応するスタンプIDとIncrとが合成される。またこのとき、電子印鑑100Bは、スタンプID等を合成する前の静止画像（或いは動画像でもよい）を自装置内に保存する。

【0084】

次に、電子印鑑100Aと電子印鑑100Bは、互いに静止画像を交換し合う。具体的には、電子印鑑100Aは静止画像Viaを電子印鑑100Bに送り、電子印鑑100Bは静止画像Vibを電子印鑑100Aに送る。

【0085】

次に、電子印鑑100Aを使用する当事者Aにより、液晶表示部107に表示された静止画像Vibに含まれるIncrBが参照され、これに対応する数値が操作部101を用いて入力されると、電子印鑑100Aはこの入力された数値を電子印鑑100Bに送る。並行して、電子印鑑100Bを使用する当事者Bにより、液晶表示部107に表示された静止画像Viaに含まれるIncrAが参照され、これに対応する数値が操作部101を用いて入力されると、電子印鑑100Bはこの入力された数値を電子印鑑100Aに送る。これらのIncrNに対応する数値の交換は、当事者の両方が入力を完了した後に行われることが望ましい。

【0086】

次に、電子印鑑100Aは、電子印鑑100Bから送られてきたIncrBと、当事者Aにより画像を参照して手入力された上記数値とを比較して一致を確認する。一致が確認されない場合には、例えば、押印処理が無効であるとして中断され、押印処理のやり直しが要求される。

【0087】

同様に、電子印鑑100Bは、電子印鑑100Aから送られてきたIncrAと、当事者Bにより画像を参照して手入力された上記数値とを比較して一致を確認する。一致が確認されない場合には、例えば、押印処理が無効であるとして中断され、押印処理のやり直しが要求される。

【0088】

各電子印鑑ともに一致判定が得られた場合には以下の処理が継続される。

【0089】

電子印鑑100Aは、Taに自己のスタンプIDA、IncrA、Vib、相手のスタ

ンプIDB、IncrBを加えて(関連付けて)文書Tを生成し、当該Tを保存する。

【0090】

同様に、電子印鑑100Bは、Tbに自己のスタンプIDB、IncrB、Via、相手のスタンプIDA、IncrAを加えて(関連付けて)文書Tを生成し、当該Tを保存する。

【0091】

次に、上述した電子認証システムにおいて詳述した方法により、文書Tの認証処理がなされる。具体的には、電子印鑑100Aは、TaをKaにより暗号化して(Ta)Kaを作成し、これを電子印鑑100Bに送る。同様に、電子印鑑100Bは、TbをKbにより暗号化して(Tb)Kbを作成し、これを電子印鑑100Aに送る。電子印鑑100Aは、(Tb)KbをKaにより暗号化して(Tb)KbKaを作成し、これを保存するとともに電子印鑑100Bに送る。また、電子印鑑100Bは、(Ta)KaをKbにより暗号化して(Ta)KaKbを作成し、これを保存するとともに電子印鑑100Aに送る。本実施形態で使用する暗号化方式は暗号化の順序を変えても結果が同じとなる性質(可換性)をもつから、Ta=Tbであれば(Ta)KaKb=(Tb)KbKaとなるし、その逆もまた真となる性質(一意性)をもつ。各電子印鑑は、暗号化して送られたきた値と自装置に保存してある値とを比較することで、相手が同じTextを電子印鑑の内部に保存しているか否かを検証できる。

【0092】

また、こうした一連の認証動作についての履歴情報は、各電子印鑑に蓄積される。例えば、認証動作を行った日時、相手に関する情報(スタンプID、Incr、Vi等)などが履歴情報として蓄積される。

【0093】

次に、当事者のいずれか(或いは双方とも)により不正な手続きがなされた場合における検証方法について説明する。

【0094】

図5は、当事者のいずれか(或いは双方とも)が改ざん等の不正を行う状況における電子印鑑の使用時の構成例を示す図である。図示のように、電子印鑑100Aと端末装置110Aとの間又は電子印鑑100Bと端末装置110Bとの間に、改ざん装置(フィルター)130A又は改ざん装置(フィルター)130Bが挿入され、不正な手続きがなされる場合を考える。

【0095】

例えば本例では、以下のような前提のもとにシステム運営を行う。

- (1)電子印鑑は所定の機能を完全に持っており、故障のことは別に考える。
- (2)耐タンパー性、ロバストネスは保証されている。
- (3)電子印鑑を使用した人物(A、B)の特定が画像により可能である。
- (4)電子印鑑を紛失した場合は、存在する電子印鑑の判定を正しいとする。
- (5)押印済み文書は平文で、どこにでも流布される。
- (6)認証・調停を外部に求めない。
- (7)押印途中で電子印鑑を伝送装置から外すことは許されない。
- (8)電子印鑑は2つの文書を並行して押印することができない。
- (9)非対面での押印が可能である。押印は電子印鑑内に保存された文書が一致したことで完了する。
- (10)Aには改ざんの意志が無く、Bはあらゆる手投を使って改ざんを行う。どちらがAでどちらがBか不定とする。
- (11)電子印鑑を特定するためのスタンプIDは、メーカー(製造者)により一意に設定されて変化することがない。
- (12)押印・認証プロトコルをリードするのはいずれの電子印鑑でも良い。
- (13)電子印鑑の使用履歴を表すIncrNは、製造者により特定の変化をするように設定される数で、同じ数は2度と現れない。製造者は依頼があれば特定の電子印鑑が発生し得

る $Inc r N$ かどうか明らかにできる。押印／認証時に使用する暗号鍵 K は 1 シーケンスごとに異なる使い捨ての鍵である。

(14) 各電子印鑑には点灯により内部状態を表示する 5 つのランプがある。使用者はこのランプを目視することにより電子印鑑の動作内容を直接知ることが可能である。

【0096】

例えば、攻撃として電子印鑑 100B に有利となる改ざん装置 130B が使用されている場合を想定する。この改ざん装置 130B は電子印鑑間の電文を全て記録し、場合に依じて電文を改ざんし、或いはなりすましができる。改ざん装置 130B の存在がなければ、電子印鑑同士は必ず同一の文書を保存し、保存文書による認証結果が異なることはない。電子印鑑 100A の判定と電子印鑑 100B の判定が食い違ったとき、お互いが正（有効）であると主張する文書を、お互いに読み込んで判定させる手順が必要である。

【0097】

各電子印鑑のスタンプ ID と $Inc r$ とのは本システムの中で一意に保たれる。電子印鑑内で、同一の $TID (IDA + Inc rA + IDB + Inc rB)$ が打たれていて、電子印鑑内に保存されている文書はただ 1 つである。物理的には 2 つの電子印鑑にそれぞれ 1 つずつ保存される。

【0098】

改ざん装置 130B が、 $Inc rB$ として勝手な値を設定して電子印鑑 100A に送ったとしても、電子印鑑 100A から正規の電子印鑑 100B に問い合わせがあれば、電子印鑑 100B が出力したことの無い $Inc rB$ であると否定されることになる。また、メーカに改ざん装置 130B が作成した $Inc rB$ を送れば、真の電子印鑑 100B で作成された値でないことを検証できる。一方、 $Inc rA$ は電子印鑑 A で作られた値であるからメーカで正しいと判定される。

【0099】

次に、電子印鑑 B を使わないなりすましがなされた場合を考える。改ざん装置 130B が電子印鑑 100B になりすまして電子印鑑 100A との押印を試みるとき、改ざん装置 130B は $Inc rB$ として電子印鑑 100B から出力される可能性のある値を使わなければならない。しかし、 $Inc rB$ を正常な値に設定できる可能性は低い。 $Inc rB$ を正しい値とするためには、電子印鑑 B を利用するか、あるいは $Inc rB$ を過去の文書から探して利用（盗用）することでメーカを信じさせることができ、電子印鑑 A に $Inc rB$ を使って押印することができる。しかし、正規の電子印鑑 100B には、 $Inc rB$ に基づく過去の押印の事実（履歴）が残っているので、電子印鑑 100A との間における押印事実を否定することは可能である。この場合、本例では内容については電子印鑑 100A の所有者である当事者 A の言い分が正しいとされる。内容について電子印鑑 100B の所有者側が反論したい場合には、改ざん装置 130B は電子印鑑 100B に Tf を記録させる必要がある。

【0100】

当事者 B は、当事者 A が勝手に作成した文書であると反論できるが、反論するために当事者 B は $Inc rB$ は他の電子印鑑との間で使用したものであること、或いは電子印鑑 100B が出力するはずのないものであることを証明する必要がある。2 つの証明方法のいずれにも電子印鑑 100B が必要であるので、電子印鑑 100B を使わないなりすましは不可能となる。

【0101】

このように、電子印鑑 100B を使わないなりすましは無意味なので、電子印鑑 100B を使ったなりすましがなされる場合について次に説明する。改ざん装置 130B が、 $Text$ に変えて $Textf$ を電子印鑑 100B に送り込むことは、押印時の検証結果を正（有効）とすることができないので無意味である。電子印鑑 100A と電子印鑑 100B とは、改ざん装置 130B を挟んで押印するとき、 $Inc rA$ 、 $Inc rB$ としてそれぞれ自装置の発行した $Inc r$ を使うことができる。しかし、内容を両電子印鑑そろって $Textf$ とすることができない。そこで、改ざん装置 130B は、電子印鑑 100A に対

しては電子印鑑100Bであり、電子印鑑100Bに対しては電子印鑑100Aであるかのように振る舞い（動作し）、電子印鑑100Aに対してはTを、電子印鑑100Bに対してはTfをそれぞれ正当な文書として認証させようと試みる。このような動作は改ざん装置が勝手にKa、Kbを設定することでそれぞれ押印時のTの一致検証を通り抜けられるので可能である。

【0102】

次に、画像の役割を説明する。画像Vaは当事者Bがその撮像タイミングを指定するので、当事者Aが押印したという事実を当事者Bに認めさせるために使われる（押印相手の確認）。当事者Bが指示した動作に当事者Aが反応すれば、当事者Bは当事者Aを相手に押印しようとしていることを確認できる。同時に当事者AはVaを含むTに押印すれば、Vaが当事者Aの立体的な肖像を写し取ったものであることを当事者Aが認めたということになる。同様に画像内に、インサートされたTID、文書のタイトルあるいは重要な一部、電子印鑑のおかれた状況（周辺の様子）などが含まれていれば、当事者A、Bいずれもこれらを認めたとする。画像Vbも当事者A、Bに対する意味合いは同じである。改ざん装置130Bは過去の記録から現在の画像Va、Vbを作成することができない。したがって改ざん装置130Bが電子印鑑Bになりすますには電子印鑑100Bと同じ動作をしなければならない。このときIncrBについては、電子印鑑100Bから予めもらわないと後の認証時になりすましてあることがわかってしまう。しかし電子印鑑100BからIncrBをもらうと、IncrBには電子印鑑100Aとは違った過去のVaを使っている。一方、電子印鑑100AにはVa、Vbとも疑いの無い映像が記録されている。当事者Bはこれ以降、このTIDに対し電子印鑑100Bでは無く改ざん装置130Bを用いて認証に臨むこととなる。しかるに改ざん装置130Bは電子印鑑100Aとの間でTの確認をすませているので、Tの中のTextを改ざんするしかできない。押印事実そのものの破棄は可能であるが当事者Bにとって不利である。また電子印鑑100Aはインサート前の画像Vaを記録しておくので、Viaが電子印鑑100AでVaによって撮影されたことを明瞭に示すことができる。Vaは電子印鑑100Aにしか知り得ない情報であるためである。画像交換にはVia、Vibに含まれるTID（IDA、IncrA、IDB、IncrB）がTに含まれるTIDと一致していると両押印者に確認させる役割がある。

【0103】

電子印鑑100B内と異なり、改ざん装置130B内は自由に改ざんをできるので、TをTfに改ざんしたとすると、電子印鑑100Aの保存するTと矛盾することになる。どちらが正しいかはわからない。この不一致は改ざん装置130Bの入っている環境では、押印時にはわからず、認証時に判定される。

【0104】

以下、説明を簡単にするため当事者BがTfを作成し、これが正しい押印文書であると主張した場合を説明する。なお、当事者AとBが入れ替わっても同じことである。

【0105】

まず、自らが押印したことの証明について説明する（検証1）。Via、Vibを示して、自らがTIDBに電子印鑑100Aを使って押印したことを示す。認証はTIDAを電子印鑑100A、TIDBを電子印鑑100Bに示し、保存されているTを比較すれば良い。それぞれランプLiA、ランプLiBが正（有効）を示す点灯状態となる。しかし当事者Bは悪意を持つから、改ざん装置130BによってTの一部を改ざんして電子印鑑Bに送り、LiBを不正とするかもしれない。

【0106】

次に、自らが押印していないことの証明について説明する（検証2）。当事者Bは、新たに作成、あるいは既存の文書を利用して改ざんした文書Tfを作成する。この場合、認証はTfを電子印鑑100A、電子印鑑100Bにそれぞれ保存されているTと比較すればランプLiは不正と表示する。しかし当事者Bは悪意を持つから、改ざん装置130Bを作用させ、Tfに変えてTを電子印鑑100Bに送り、電子印鑑100BのランプLI

Bが正（有効）を示すようにするかもしれない。

【0107】

次に、自らも相手も押印したことの証明について説明する。上述した検証1、2により、TについてL i Aは正、T fについてL i Bが正を示す状態となった。このような状態は改ざん装置130Bが存在しているので、正しいと主張するほうが相手も確かに押印したということを示す必要がある。自分が押印していないというだけでは不十分である。この改ざん装置130Bは情報伝送手順と以下の情報、T、T f（IDA、IDB、IncrA、IncrB、Va、Vb）、Hush、（Hush）Ka、（Hush）Kb、及び認証時点以前に押印、認証に使われた情報すべてを有している。これらの情報は認証に用いると、改ざん装置130Bで改ざんされるので使えない。Ka、Kbによる暗号が掛けられている情報は、鍵が使い捨てなので安全である。

【0108】

まず、自己認証、すなわち電子印鑑の内部の情報との一致判定について説明する。当事者A、Bは、それぞれ自らが正しいと主張する2つの文書T、T fを電子印鑑100A、電子印鑑100Bにそれぞれに送り、Ta、Tbとして保持する（Ta=T、Tb=T f）。同様に相手が正しいと主張する2つの文書T f、Tを電子印鑑100A、電子印鑑100Bにそれぞれに送り、Taj、Tbjとして保持する（Taj=T f、Tbj=T）。

【0109】

電子印鑑100Aは、内部に蓄積したデータTにより、受け取ったデータTa、Tajのどちらに自分が押印したことが有るか検査する。電子印鑑100AはまずTa、Tajにそれぞれ含まれているIDA、IncrA、IDB、IncrBを検索キーにして、電子印鑑の内部の文書に一致するか検査する。電子印鑑100Bも同じ動作を行う。このとき両者が自らの文書が正しいと主張する以上、Ta=T、Tbj=Tとなり、ランプL i Aと電子印鑑100BのランプL i Bが正の表示をするはずである。さらに、L j A、L j Bが正の表示となればT=T fであり、これ以上の認証は不要である。読込判定時の解釈を以下の表1に示す。

【0110】

【表1】

| ケース | L i A | L j A | L i B | L j B | 判定 |
|-----|-------|-------|-------|-------|-------------------------------------|
| 1 | ○ | ○ | ○ | ○ | T=T fと判定 |
| 2 | ○ | × | × | ○ | Ta=Tと判定、Aが正しいと判定 |
| 3 | × | ○ | ○ | × | Tb=Tと判定、Bが正しいと判定 |
| 4 | ○ | × | ○ | × | 不正操作（フィルタ操作n）の可能性あり。 認証が必要。 |
| 5 | ○ | — | × | — | ケース2以外ではB側で不正操作の可能性あり。 Tが正と判断。 |
| 6 | × | — | ○ | — | ケース3以外ではA側で不正操作の可能性あり。 T fが正と判断。 |
| 7 | × | — | × | — | 不正操作の可能性あり。 Ta、T fとも不正と判定。 |
| 8 | × | × | × | × | Ta、Taj、Tb、Tbjとも押印 したことはない。 |

上記表1では、各状況（ケース1、2、3…）におけるランプL i A等の点灯状態（点灯が「○」、不点灯が「×」、点灯／不点灯を不問の場合が「—」）と、それらの点灯状

態の組み合わせによる判定結果が示されている。例えば、各ランプの点灯状態がケース1に示す状態である場合には、 $T = T f$ との判定結果が得られる。各ランプの点灯状態がケース2に示す状態である場合には、 $T a = T$ であり当事者Aの言い分が正しいとの判定結果が得られる。各ランプの点灯状態がケース3に示す状態である場合には、 $T b = T$ であり当事者Bの言い分が正しいとの判定結果が得られる。各ランプの点灯状態がケース4に示す状態である場合には、改ざん装置130A及び／又は改ざん装置130Bの挿入による不正操作の可能性がある、互いの文書について更に認証処理を行う必要があるとの判定結果が得られる。各ランプの点灯状態がケース5に示す状態である場合には、上記ケース2に該当する場合以外には、当事者B側で改ざん装置130Bの挿入等による不正操作の可能性がある、Tが正しい文書であるとの判定結果が得られる。各ランプの点灯状態がケース6に示す状態である場合には、上記ケース3に該当する場合以外には、当事者A側で改ざん装置130Aの挿入等による不正操作の可能性がある、Tfが正しい文書であるとの判定結果が得られる。各ランプの点灯状態がケース7に示す状態である場合には、当事者A、Bの双方の側で改ざん装置130A又は130Bの挿入等による不正操作の可能性がある、T及びTfのいずれも正しい文書ではないとの判定結果が得られる。各ランプの点灯状態がケース8に示す状態である場合には、当事者A、Bの双方ともに、文書Ta、Taj、Tb、Tbjのいずれに対しても電子印鑑を用いて押印した事実が存在しないとの判定結果が得られる。

【0111】

次に、電子印鑑同士の相互認証（情報交換による認証）について説明する。この場合、不正な目的で設置される改ざん装置の存在を考慮したうえでどちらの主張が正しいか検査しなければならない。例えば、当事者Bが不正な目的をもって改ざん装置130Bを電子印鑑100B側に設置した場合、次のような状況が発生する。改ざん装置130Bが可能な動作は以下の表2に示す通りである。なお、当事者Aが不正な目的をもって改ざん装置130Aを設置した場合も同様である。

【0112】

【表2】

| 不正操作 | Ai | Aj | Bi | Bj | LiA | LjA | LiB | LjB | Bにとって効果 |
|--------------------------------------|----|----|----|----|-----|-----|-----|-----|------------|
| Bに対して $T \longleftrightarrow T f$ | T | Tf | T | Tf | ○ | × | ○ | × | 有り。認証が必要。 |
| B $T f \rightarrow T$ | T | Tf | T | T | ○ | × | ○ | ○ | 無し（Tを正と判定） |
| B $T \rightarrow T f$ | T | Tf | Tf | Tf | ○ | × | × | × | 無し（Tを正と判定） |
| Aに対して $T f \rightarrow T$ | T | T | Tf | T | ○ | ○ | × | ○ | 無し（Tを正と判定） |

改ざん装置130Bが、TをTfに入れ替える（ $T \longleftrightarrow T f$ ）処理を行った場合に、当事者AとBのどちらが不正目的の改ざん装置を設置しているかは、認証が終わるまでわからない。当事者Bによる押印そのものの否定は、当事者AがIDA、IncrA、IDB、IncrBに基づいて自己の電子印鑑100Aに蓄積した履歴情報の中から探し出した画像を視認することで確認が行われる。システムとして必ずしも本人認証を保証し得るものではないが、画像は真正なものであることが保証されるので、補強情報として利用できる。

【0113】

（ステップ1：データ交換）

電子印鑑100AはTaを自らが生成する使い捨て暗号鍵Kaにより暗号化して（Ta）Kaを作成し、電子印鑑100Bに送る。また、電子印鑑100BはTbを自らが生成

する使い捨て暗号K bにより暗号化して(T b) K bを作成し、電子印鑑1 0 0 Aに送る。改ざん装置1 3 0 BはK a、K bを知らないで、(T a) K a、(T b) K bに代えて正しい(T a) K a、(T b) K bを作ることができない。改ざん装置1 3 0 Bができるのは伝送データを電子印鑑が不正であると判定するように改ざんすることだけである。電子印鑑1 0 0 Aは(T a) K b K aを作成し、また電子印鑑1 0 0 Bは(T b) K a K bを作成し、その後お互いに(T a) K b K aと(T b) K a K bを交換する。両方のデータが一致すればT a=T bであると電子印鑑1 0 0 A、電子印鑑1 0 0 Bの双方が認証したことになる。ランプL j A、ランプL j Bがともに「正」状態に表示されるが、T a=T b=Tが証明されたわけではない。しかしステップ1を省略すると電子印鑑1 0 0 Bは、電子印鑑1 0 0 A側から「改ざん装置を入れているのではないか」との指摘がなされるとこれに反論できない。ステップ1は、当事者A側の、TをT fに入れ替える(T \longleftrightarrow T f)操作は確実であると当事者Bに認めさせる効果がある。

【0114】

(ステップ2：T a j \neq T bであることを確認)

T a jを使用してステップ1の処理を行う。T a j=T fが送られたとき、L i Bが「正」を示すはずである。しかし、L j Bが「不正」を表示しても当事者Bの抱く疑いに対して反論できない。なお、本ステップの処理は省略も可能である。

【0115】

(ステップ3：T a=Tであることを検査)

電子印鑑1 0 0 Aは、内部に保存していたTよりステップ1の処理を行う。このとき電子印鑑1 0 0 Bが主張するように、仮に電子印鑑1 0 0 A側に改ざん装置1 3 0 Aが存在し、T aにT fを書き込んでいれば、Tを送ったとき、かならずL j Bは不正を示すはずである。T a=T b=T、従って、T b=T \neq T fであり、電子印鑑1 0 0 Bが正しくT fを読み込んでいることが否定される。電子印鑑1 0 0 B側に設置された改ざん装置1 3 0 Bはこれを予想してL j Bを不正とするような動作をする。

【0116】

T aまたはTを明示的に送っていると、改ざん装置が動作している可能性がある。そのためステップ1においてランダムにT aとTを送る。このときどちらを送ったか電子印鑑1 0 0 Aは外部に出さない。電子印鑑1 0 0 BはT aとT bのどちらが送られてきたかわからない状態で、L j Bの状態を電子印鑑1 0 0 Aに伝える。電子印鑑1 0 0 Aは、L f Aの状態は、Tを送った時に、L j Bが正を表示したことを示し、お互いに(T) K b K a、(T f) K a K bを交換して等しくなるか確かめる。この時、T a=T b=Tが確認される。この場合は、メーカーに電子印鑑1 0 0 Aと改ざん装置1 3 0 Bのどちらがなりすましを行っているか検証してもらうこととなる。電子印鑑1 0 0 Aはメーカーの疑問を呼ばない。改ざん装置1 3 0 Bはメーカーの質問に答えるために電子印鑑1 0 0 Bの助けを借りる必要がある。メーカーの質問は、電子印鑑1 0 0 Bしか復号できないK t bを用いて行われる。改ざん装置はメーカーによる検査の期間どうしても電子印鑑1 0 0 Bを接続しておかなければならない。このときメーカーが当該T I Dを持つTを出力させる要求を行うと電子印鑑1 0 0 Bは該当するT I Dが入っていないので答えられない。改ざん装置1 3 0 Bはこの質疑を察知できず、電子印鑑1 0 0 Bの回答を自らが蓄積しているT I Dに置き換えられない。

【0117】

第三者認証機関を利用すれば、公開鍵を使って、認証や伝送路の暗号化を行えるが、第三者の介入無しに契約文書の認証を行う場合、本実施形態のシステムは有効である。暗号化無しでは二者間で正しい押印認証が行えない。二者間で公開鍵方式を使うことにより文書の認証を行うことが可能であるが、この場合、どちらかに主導権があり、対等な状態での判定はできない。共通鍵方式では、全部の電子印鑑が同じ鍵を使うので、一度鍵が盗まれるとシステムが崩壊するおそれがある。本方式の認証は使い捨ての鍵しか使わず、システムが崩壊する可能性はきわめて低い。本方式でもI n c r Nの正当性を電子印鑑のメーカーに依存するので、全く第三者の介入が無いわけではないが、一方が特定の方法でなりす

ましを行った場合のみメーカに検証を依頼すればよいので、大部分のトラブルについては二者間で解決できる。

【0118】

本実施形態のシステムの特徴をまとめると以下のようになる。

(1) 当事者Bの否定に対する当事者Aの反論

電子印鑑の使用についての否定（押印の否定）については、V b i の提示によりこれを覆すことができる。

(2) T e x t f の否定

文書番号の否定については、T I D B による電子印鑑1 0 0 B の検索により、これを覆すことができる。

(3) 電子印鑑1 0 0 A、電子印鑑1 0 0 B のもつ秘密

これから発生する未来のI n c r N について、電子印鑑のメーカだけが知り得る。

(4) 誰も知り得ない事項

暗号鍵K i n c r、インサート（合成）前の自分の画像については誰も知り得ない。

(5) 改ざんできない内容

T I D をインサート（合成）後の画像については改ざんできない。

(6) 不変が保証されるもの

各電子印鑑のスタンプI D（I D A、I D A b）、各電子印鑑内に保存される文書T については不変であることが保証される。

(7) 排除が保証されているもの

T I D A は電子印鑑1 0 0 A、1 0 0 B 内の調印文書にでてくるのはただ1 つである。T I D B も電子印鑑1 0 0 A、1 0 0 B 内の調印文書にでてくるのはただ1 つである。

(8) その他

I D A、I n c r A、I D B、I n c r B が各電子印鑑の内部に保存された画像V a i、V b i の上でそろふことは、少なくとも電子印鑑1 0 0 A、電子印鑑1 0 0 B が利用されたことを示している（証明できる）。

【0119】

なお、本発明は上述した実施形態の内容に限定されるものではなく、本発明の要旨の範囲内において種々の変形実施が可能である。

【図面の簡単な説明】

【0120】

【図1】 本発明を適用した一実施形態の電子認証システムの構成を説明する図である。

【図2】 電子認証システムにおける認証処理の手順を説明するフローチャートである。

【図3】 電子印鑑の具体例について説明する図（斜視図）である。

【図4】 当事者のいずれも改ざん等の不正を行わない正常な状況における電子印鑑の使用時の構成例を示す図である。

【図5】 当事者のいずれか（或いは双方とも）が改ざん等の不正を行う状況における電子印鑑の使用時の構成例を示す図である。

【符号の説明】

【0121】

1…第1の装置

2…第2の装置

1 0、2 0…制御部

1 1、2 1…暗号化処理部

1 2、2 2…記憶部

1 3、2 3…認証処理部

1 4、2 4…通信処理部

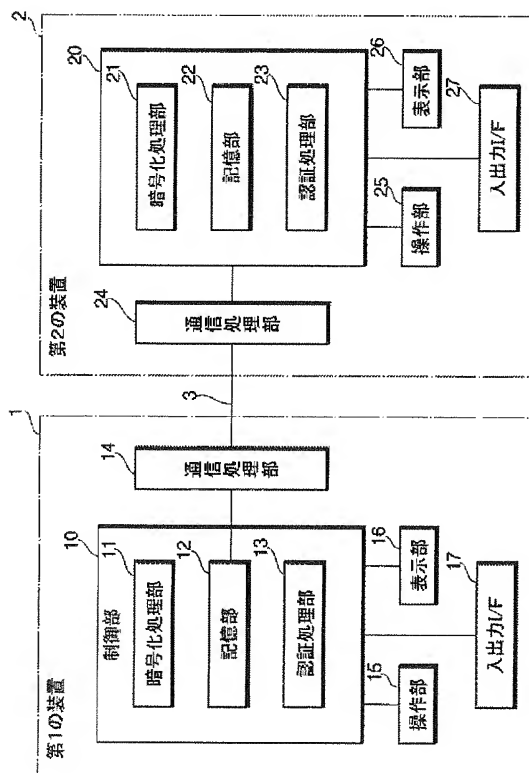
1 5、2 5…操作部

1 6、2 6…表示部

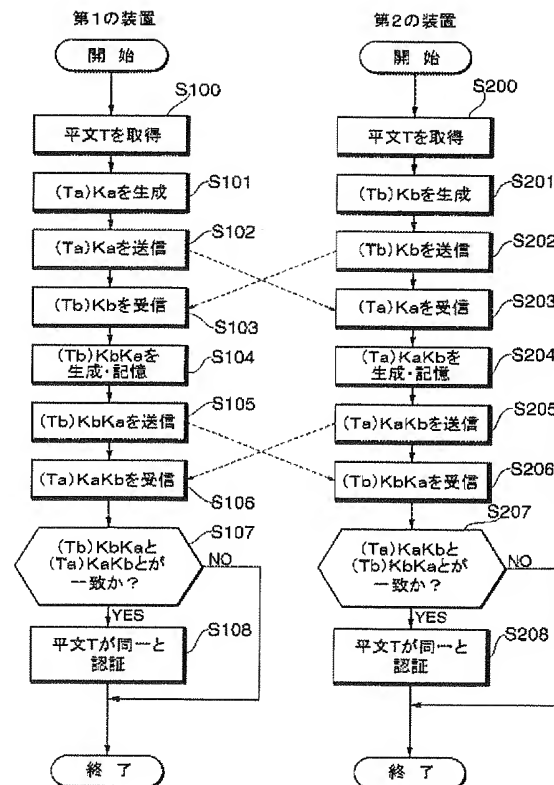
1 7、2 7…入出力インタフェース

- 100、100A、100B…電子印鑑
 101…操作キー（数字キー）
 102～105…ランプ
 106…カメラユニット
 107…液晶表示部
 108…入出力インタフェース

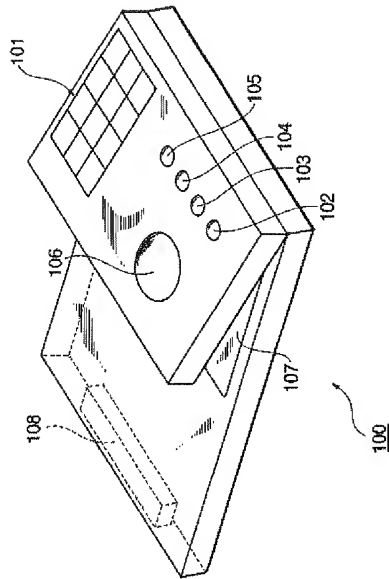
【図1】



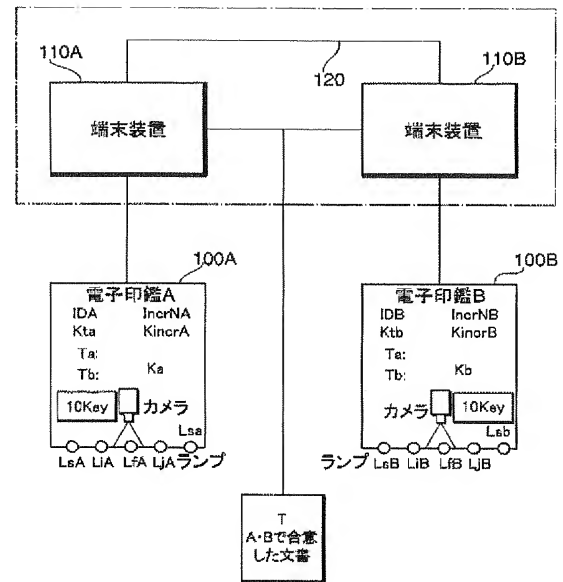
【図2】



【図3】



【図4】



【図5】

